

10/583356

1

AP3 Rec'd PCT/PTO 19 JUN 2005

PROCEDE DE DETECTION DE MODIFICATIONS ILLICITES DES LOGICIELS CONSTRUCTEURS

L'invention concerne notamment un procédé permettant de détecter des modifications et/ou d'éviter la modification de logiciels constructeurs pour mobile GSM (abréviation anglo-saxonne de Global System Mobile), logiciels embarqués dans une mémoire reprogrammable.

5 Elle concerne aussi tout système comportant un noyau dur (hardware non modifiable se présentant sous la forme d'un ASIC par exemple) et un noyau mou (comprenant des fonctions de sécurité programmables), par exemple un ordinateur de type PC comprenant un ASIC non reprogrammable et un système d'exploitation.

10

Les terminaux mobiles GSM sont reprogrammables afin de pouvoir faire évoluer les versions logicielles des services offerts aux utilisateurs. Actuellement, l'accès aux fonctions de reprogrammation n'est pas suffisamment sécurisé et certains utilisateurs parviennent facilement à
15 effectuer des modifications logicielles afin d'outrepasser les fonctions de sécurité intégrées par les constructeurs. De ce fait, ils falsifient le fonctionnement des terminaux afin d'accéder à des fonctions ou des services supplémentaires ou de réutiliser des terminaux volés.

Les moyens de protection actuels contre les modifications illicites
20 de logiciels sont insuffisants. Les pirates parviennent assez rapidement à trouver les adresses des mémoires programmables à modifier, pour neutraliser ou contourner les mécanismes de sécurité mis en place par les constructeurs. L'objectif des « pirates » est d'autoriser, sans paiement, l'accès aux services supplémentaires potentiellement disponibles et
25 d'outrepasser les contrôles d'accès.

Les modifications sont réalisables via de multiples canaux (UART ou Universal Asynchronous Receiver/Transmitter, USB ou Universal Serial Bus, JTAG ou Joint Test Action Group,...) ou par modification directe sur la

mémoire reprogrammable ou FEPRM (Flash Erasable Programmable Read Only Memory), par atteinte à l'intégrité matérielle par dé soudage – re soudage, par exemple.

Le mode actuel de démarrage d'un terminal GSM en mode auto-configuration, par détection de signaux spécifiques, est un mécanisme faible qui n'offre pas de protection solide.

L'invention concerne un procédé permettant de détecter et/ou d'éviter la modification de logiciels embarqués dans une mémoire reprogrammable au sein d'un système comprenant un noyau dur contenant des fonctions de sécurité matérielle adaptées à vérifier l'intégrité notamment d'un noyau mou comprenant une mémoire reprogrammable, le système comportant une interface locale de données. Il est caractérisé en ce qu'il comporte au moins les étapes suivantes :

A1 – le signal reçu sur l'interface locale de données n'est pas valide, mettre le système dans un état non opérationnel,

B1 – le signal reçu est un signal de déconnexion sur l'interface locale de données, ou il n'y a pas de signal, lancer une procédure de démarrage sécurisé, avec exécution des fonctions de contrôle :

Autotest du noyau dur :

- Si l'autotest est OK, alors tester l'intégrité de la mémoire reprogrammable,
 - Si cette intégrité est OK, alors activer le système pour un fonctionnement normal
 - Si cette intégrité est KO, alors mettre le système dans un état non opérationnel

Si l'autotest est KO, alors mettre le système dans un état non opérationnel,

C1 – le signal reçu est un signal de démarrage valide,

- Si le système est dans un mode de développement, le rendre opérationnel,

- Si le système est dans un mode d'exploitation opérationnelle et si le signal est un signal de test, alors désactiver au moins une des fonctions essentielles du fonctionnement opérationnel.

L'invention concerne aussi un procédé permettant de détecter
5 et/ou d'éviter des modifications illicites d'un logiciel constructeur au sein d'un système de type GSM, comprenant un noyau dur et un noyau mou, une interface locale de données, caractérisé en ce qu'il comporte au moins les étapes suivantes :

A2 – le signal reçu sur l'interface locale de données du terminal n'est pas
10 valide, mettre le terminal GSM dans un état non opérationnel,

B2 – le signal est un signal de déconnexion sur l'interface locale de données ou il n'y a pas de signal, lancer une procédure de démarrage sécurisé, avec exécution des fonctions de contrôle :

Autotest du noyau dur

- 15 • Si l'autotest est OK, alors tester l'intégrité du noyau mou
 - Si cette intégrité est OK, alors activer le terminal pour un fonctionnement normal,
 - Si l'intégrité est KO, alors mettre le terminal dans un état non opérationnel,
- 20 • Si l'autotest est KO, alors mettre le terminal GSM dans un état non opérationnel.

C2 – le signal reçu est un signal de démarrage valide :

- Si le fusible est non claqué, rendre le terminal GSM opérationnel,
- Si le fusible est claqué, rendre le terminal non totalement opérationnel,
25 en désactivant au moins une des fonctions opérationnelles du terminal :
 - o Si le signal est un signal de type test JTAG, poursuivre la procédure de test,
 - o Si le signal est un signal de test, démarrer en mode non
30 sécurisé et poursuivre la procédure de test.

L'échange des données entre le noyau dur et le noyau mou est par exemple effectué en utilisant un algorithme basé sur le principe de non-rejeu et de non prédictibilité des données transmises.

L'invention concerne aussi un système permettant de détecter
5 et/ou d'éviter la modification de logiciels embarqués dans une mémoire programmable comprenant un noyau dur contenant des fonctions de sécurité matérielle et un noyau mou comprenant une mémoire programmable, une interface locale de données apte à recevoir des signaux. Il est caractérisé en ce qu'il comporte des moyens adaptés à :

- 10 ➤ mettre le système dans un état non opérationnel lorsque le signal reçu sur une interface locale de données n'est pas valide,
- pour un signal reçu de déconnexion ou absence de signal sur une interface locale de données, lancer une procédure de démarrage sécurisé, avec exécution de fonctions de contrôle :

15 Autotest du noyau dur :

- Si l'autotest est OK, alors tester l'intégrité de la mémoire programmable,
 - 20 ○ Si cette intégrité est OK, alors activer le système pour un fonctionnement normal
 - Si cette intégrité est KO, alors mettre le système dans un état non opérationnel
- Si l'autotest est KO, alors mettre le système dans un état non opérationnel,
 - 25 ➤ Pour un signal reçu est un signal de démarrage valide,
- Si le système est dans un mode de développement, le rendre opérationnel
- Si le système est dans un mode d'exploitation opérationnelle, et si le signal est un signal test alors désactiver une des fonctions essentielles du fonctionnement opérationnel au démarrage.

30

Le système peut comporter des moyens de sécurisation des échanges de données entre le noyau dur et le noyau mou.

Le système peut être un terminal GSM ou un micro-ordinateur de type PC ou un lecteur de type MP3 contenant une mémoire reprogrammable.

Le procédé selon l'invention présente notamment les avantages
5 suivants. Il tient compte du processus industriel de production, de commercialisation et de maintenance. L'adaptation des principes d'intégrité (au sens authenticité : origine et intégrité), des logiciels et données reprogrammables est répartie sur des dispositifs matériels intégrés dans un ASIC garantissant la non modification des mécanismes de contrôle, associés
10 à des dispositifs de sécurité logiciels adaptables aux différentes versions logicielles de terminaux GSM par exemple.

D'autres caractéristiques et avantages de l'invention apparaîtront mieux à la lecture de la description d'un exemple donné à titre illustratif et
15 nullement limitatif annexé des figures qui représentent :

- La figure 1 les composantes fonctionnelles d'un terminal mobile GSM ayant un impact sur la sécurité d'accès,
- La figure 2 la structure de la FEPRM,
- La figure 3 trois niveaux de sécurité considérés lors du démarrage du
20 GSM,
- La figure 4 un schéma de la logique de l'ensemble,
- La figure 5 un exemple d'échanges sécurisés entre composants du terminal GSM sans secret partagé.

25 Afin de mieux faire comprendre le principe du procédé selon l'invention, l'exemple qui suit est donné pour un système GSM dont l'architecture est rappelée à la figure 1.

Cette figure 1 représente l'architecture fonctionnelle d'un terminal GSM structuré en plusieurs modules. Seuls les modules ayant un impact sur
30 la sécurité sont représentés sur cette figure et sont pris en compte pour la description. On distingue une composante matérielle comprenant le noyau dur et une composante logicielle comprenant le noyau mou. Le noyau dur

correspond aux fonctions de sécurité matérielles qui permettent de vérifier l'intégrité du terminal lors d'un démarrage normal ou de rendre non-opérationnel le terminal GSM dans tout autre mode de fonctionnement. Le noyau mou intègre les fonctions de sécurité logicielles qui assurent la sécurité du code chargé en FEPRM. Le noyau mou est signé hors ligne par une clé secrète, et sa signature est vérifiée lors du démarrage NORMAL par le noyau dur. En cas de compromission constatée de l'intégrité du terminal GSM (perte de l'intégrité du noyau mou), le terminal devient non-opérationnel pour tout mode de démarrage jusqu'à ce qu'un nouveau noyau mou intègre soit téléchargé dans le terminal.

Les deux modules pris en compte dans la suite de la description sont :

la composante matérielle comprenant :

- Le module ECOUTE_SIGNAL ;
- Le module DESACTIVATION_FONCTION ;
- Le module DEMARRAGE ;
- Le module NOYAU_DUR ou module de sécurité matérielle.

la composante logicielle comprenant :

- Le module NOYAU_MOU ; où module de sécurité logicielle ;
- Le module APPLICATIONS.

Le module APPLICATIONS de la composante logicielle est partiellement sécurisé. Il dépend étroitement de la politique de sécurité choisie par le constructeur.

Ces deux composantes sont détaillées dans la suite de la description.

La description adopte la terminologie suivante :

VAR : une variable ou un état non souligné traduit son caractère ACTIF ;

VAR : une variable ou un état souligné traduit une NEGATION de son caractère ACTIF.

Composante matérielle

NOYAU_DUR

Le noyau dur contient les mécanismes de sécurité matériels qui permettent de vérifier son bon fonctionnement et l'intégrité du noyau mou et les mécanismes qui permettent de définir la politique de sécurité à appliquer en fonction du mode de démarrage (JTAG, AUTRE, NORMAL), et la phase
5 de fonctionnement du terminal, ASIC avec bit claqué ou non.

Vu de la sécurité, les fonctionnalités couvertes par les différents modules de la composante matérielle sont implémentées en deux versions de composants :

Le Composant FUSIBLE NON CLAQUE (aucune activation de
10 mécanismes de sécurité) qui utilise les modules suivants :

- ECOUTE_SIGNAL
- FUSIBLE
- DEMARRAGE non sécurisé

Le Composant FUSIBLE CLAQUE qui comporte deux modes de
15 fonctionnement selon la détection ou non d'un signal au démarrage du terminal (Module ECOUTE_SIGNAL) (signal observé au niveau de l'interface locale de données du terminal GSM)

- Absence de signal : mode de démarrage sécurisé (le terminal est opérationnel)

20 ECOUTE_SIGNAL
FUSIBLE
DEMARRAGE (SECURISE)

- Réception d'un signal au niveau de l'interface locale de données du terminal GSM : activation de la fonction SPLIT (inhibition d'une
25 fonction essentielle rendant le terminal non opérationnel)

ECOUTE_SIGNAL
FUSIBLE
DESACTIVATION_FONCTION (ou SPLIT)
DEMARRAGE (NON-SECURISE)

Module ECOUTE_SIGNAL

Ce module permet de connaître le type de signal reçu au niveau de l'interface locale de données du terminal GSM. Il peut s'agir d'un signal de

5 type :

- JTAG : mode de démarrage de test où la composante d'amorçage du système ou en anglo-saxon BOOT n'est pas réveillée, la partie sécurité n'est donc pas activée,
- 10 • NORMAL : mode de fonctionnement nominal (aucun signal reçu au démarrage du terminal) où la sécurité est systématiquement activée lorsque le bit est claqué,
- REDEMARRAGE : réinitialisation du système dans un état stable avant redémarrage à froid avec des paramètres prédéfinis,
- 15 • AUTRE : mode de démarrage correspondant à divers modes de TEST où la composante BOOT est réveillée mais la partie sécurité n'est pas activée.

La réception d'un signal sur l'interface locale de données du terminal GSM doit conduire à basculer systématiquement le terminal dans un
20 mode non opérationnel si le fusible est claqué, avec une désactivation du clavier, du son ou d'une fonction essentielle par exemple.

MODULE DESACTIVATION_FONCTION (ou SPLIT)

Ce module permet de rendre le terminal non opérationnel par désactivation d'une fonction essentielle au fonctionnement du terminal GSM,
25 par exemple le clavier, le son ou autre. Ce module est appelé MODULE SPLIT dans un souci de simplification des figures.

MODULE FUSIBLE

Ce module permet de tester l'état du fusible qui correspond :
30 NON CLAQUE, au mode de développement avant vente (développement, débogage...), avec l'utilisation de la version ASIC comportant un fusible non claqué.

CLAQUE au mode d'exploitation du terminal GSM, après mise dans le circuit de vente, avec l'utilisation de la version ASIC comportant un fusible claqué.

MODULE DEMARRAGE

- 5 Ce module a notamment pour fonction d'activer la politique de sécurité en fonction du type de démarrage sollicité et permet d'appliquer la politique de sécurité selon l'état du fusible et la présence ou non d'un signal.

MODULES PILOTES

- 10 Ce module permet de charger les pilotes FLASH, de gestion des E/S, afin de lire, écrire et exécuter en FEPRM. Les modules Hardware ECOUTE_SIGNAL et FUSIBLE_CLAQUE sont enfouis dans le composant ASIC, il n'est pas possible d'écouter ou intercepter les flux échangés entre les deux composantes.

15

Composante logicielle

La figure 2 représente la structure de la FEPRM (abréviation anglo-saxonne de Flash Programmable Read Only Memory) et son interaction avec le noyau dur.

- 20 *MODULE NOYAU_MOU*

- Le noyau mou est une surcouche applicative qui assure notamment la sécurité des applications et des données sensibles référencées dans la liste des éléments sensibles à protéger. Les mécanismes de sécurité du noyau mou sont mis en œuvre au niveau de la
- 25 FEPRM après exécution du noyau dur.

La modification du noyau mou nécessite une phase de téléchargement d'un nouveau noyau mou signé afin que ce dernier soit reconnu comme valable au niveau du noyau dur.

MODULE APPLICATIONS

- 30 Ce module peut disposer de mécanismes de sécurité, répartis dans l'ensemble du code contenu en FEPRM, dont l'objectif principal est de détecter toute modification intempestive de l'intégrité du code sensible

surveillé. Les mécanismes de sécurité de ce module sont spécifiques des fonctions constructeur intégrées en FEPRM.

L'idée de l'invention repose notamment sur le contrôle du
5 téléchargement de logiciels dans la FEPRM. Cette sécurisation est basée sur un contrôle d'authenticité et d'intégrité des logiciels à télécharger.

Pour cela, le procédé prend en compte le cycle de vie complet des terminaux. Ce cycle de vie correspond aux phases de développement matériels et logiciels, intégration, tests, validation, mise en service,
10 exploitation, tests d'investigation en cas de dysfonctionnement, retour en maintenance avec possibilité d'effectuer des modifications directes du code logiciel ou patches, pour permettre de tester et de valider les corrections d'erreurs ou l'intégration d'évolutions.

Une partie des mécanismes proposés dans le procédé selon
15 l'invention est basée sur l'utilisation de mécanismes de signature utilisant un algorithme de Hash et de chiffrement asymétrique. Ceci permet notamment de ne pas être contraint par la divulgation inopinée d'information secrète. En effet, seul le signataire possède la clé secrète, la clé permettant les contrôles d'authenticité et d'intégrité est une clé publique.

20 Cette opération de signature est effectuée, par exemple, après validation des logiciels sur une station dédiée avant diffusion des logiciels à télécharger. Seule cette station aura la connaissance de la clé secrète de signature. Cette station aura également la capacité de générer les paires de clés asymétriques en cas de besoin de renouvellement des clés.

25 Le procédé selon l'invention concerne les mécanismes de sécurité matérielle pris en considération à la conception du terminal mobile et aussi les mécanismes de sécurité à ajouter au niveau de la couche logicielle du terminal.

Dans la suite, de la description on fait intervenir deux modes de
30 fonctionnement :

Le Mode NORMAL : ce mode permet d'activer les procédures de démarrage de l'ASIC du terminal GSM et de rendre opérationnel le terminal GSM,

Le Mode TEST : ce mode permet potentiellement d'outrepasser les procédures de démarrage de l'ASIC (par exemple en utilisant l'interface JTAG) et de lire et/ou d'écrire directement en FEPRM.

Il est prévu deux états de fonctionnement pour la mise en service des
5 mécanismes de sécurité selon l'état du fusible décrit ci-après. L'état du fusible correspond à une version d'ASIC spécifique.

La figure 3 schématise différents niveaux de sécurité qui seront détaillés à la figure 4 du schéma de logique d'ensemble.

10 Trois cas sont à considérer lors du démarrage du terminal, figure 3 :

Fusible non claqué, avec ou sans signal

Ce cas concerne tout type de démarrage avec ou sans signal dès lors que le fusible est claqué ; les mécanismes de sécurité ne sont pas activés

Signal et Fusible claqué

15 Ce cas met en œuvre l'activation de la fonction SPLIT

Pas de signal et Fusible claqué

Le démarrage est sécurisé

Pas de signal et fusible non claqué

Le démarrage n'est pas sécurisé

20 La figure 4 détaille les différentes étapes mises en œuvre par le procédé selon l'invention.

Le terminal GSM étant dans un état éteint, le procédé vérifie s'il reçoit un signal sur l'interface locale de données (signal externe par opposition à l'allumage habituel du GSM).

25

A2 – Dans le cas où le signal reçu n'est pas valide, alors le procédé bascule le terminal GSM dans un état non opérationnel (action = extinction).

B2 – Dans le cas où le terminal GSM ne reçoit pas de signal ou reçoit un signal de déconnexion sur l'interface locale de données, on se trouve dans le
30 mode NORMAL → allumage en mode d'exploitation normal. Le procédé lance alors la procédure de démarrage sécurisé, (toutes les procédures de sécurité intégrées sont activées normalement, en cas d'atteinte constatée de perte en intégrité du système, le terminal n'est plus opérationnel)

Après allumage, le procédé exécute ensuite les fonctions de contrôle :

Autotest du noyau dur :

- Si l'autotest est OK, alors on teste l'intégrité du noyau mou
 - Si cette intégrité est OK, alors le terminal peut être activé pour un fonctionnement normal,
 - Si l'intégrité est KO, alors le système GSM est mis en état non opérationnel.

Dans ce mode, le terminal est apte à détecter une intrusion et donc à réagir à toute modification des zones sensibles. Dans le cas de la détection de perte d'intégrité du noyau mou, le terminal GSM exécute les fonctions de défense prévues.

- Si l'autotest du noyau dur est KO, alors le terminal GSM est mis dans un état non opérationnel.

C2 – Dans le cas où le terminal GSM reçoit un signal de démarrage valide alors le procédé exécute les étapes suivantes :

- Le fusible est non claqué, Auto-configuration NON CLAQUE, aucune fonction de sécurité n'est mise en œuvre, le système est rendu opérationnel (état allumé, attente action).
- Le fusible est claqué, Auto-configuration CLAQUE, le terminal est rendu non totalement opérationnel en utilisant une fonction de SPLIT, alors
 - Si le signal est un signal JTAG, on désactive le clavier ou l'écran, avant de poursuivre la procédure de test,
 - Si le signal est un autre signal de test valide, on désactive le clavier ou l'écran, et on lance une procédure de démarrage non sécurisée avant de poursuivre la procédure de test,

Ces deux modes de désactivation complémentaires et disjoints permettent notamment de dérouler tous les scénarios de tests sans que le terminal ne soit complètement opérationnel.

Il est possible, par exemple, de définir un mode de désactivation où une interface utilisateur serait déportée du terminal GSM.

Par exemple, pour une interface clavier :

- Mode test 1 : le terminal est opérationnel mais le clavier est inactif. Ce mode requiert l'ajout d'un clavier déporté sur la machine test.
- Mode test 2 : le clavier est opérationnel – la voie radio ou toute autre fonction est inactive.

5

La figure 5 schématise les principes de sécurisation des échanges de message entre les modules du terminal GSM.

La sécurisation des échanges de données est par exemple basée sur les principes de non-rejeu des données transmises et de non prédictibilité
10 des données dynamiques.

Il peut être envisageable d'implémenter l'un ou l'autre des mécanismes au niveau du terminal GSM. L'ajout d'une donnée dynamique (valeur temporelle ou pseudo-aléa) pour rendre dynamiques les échanges de messages afin de limiter toute tentative de rejeu d'un flux intercepté ou
15 d'utilisation de logiciels piratés.

Le composant A peut être l'ASIC (où il y a le NOYAU DUR) et le composant B peut être la FEEPROM (où il y a le NOYAU MOU). Les échanges entre A et B sont alors protégés par le processus décrit sur la figure 5. SHA représente une fonction de "hachage", XOR correspond à une opération "ou
20 exclusif", DYN correspond à une chaîne aléatoire.

Les messages échangés sont par exemple les suivants :

- 1/ Générateur de données dynamiques (horloge, pseudo-aléa) -> DYN
 - 25 De l'ASIC A vers la FEPROM
 - 2/ Envoi de DYN
 - 3/ $MSG_1 = SHA(DYN \text{ reçu}) XOR Question$
- de la FEPROM B vers l'ASIC A

4/ Envoi de MSG1

5/ *Question reçue* = SHA(DYN) XOR(MSG1)

6/ Vérification de la sémantique de la question reçue

7/ $MSG2 = SHA(Question\ reçue, DYN) XOR\ REPONSE$

5 de l'ASIC A vers la FEPRM B

8/ Envoi de MSG2

9/ $REPONSE_RECUE = MSG2 XOR SHA(Question, DYN\ reçu)$

10 Sans sortir du cadre de l'invention, le procédé s'applique aussi pour détecter et/ou éviter les modifications illicites au sein d'un système de type PC, comprenant un ASIC, (hardware non modifiable) et un espace mémoire comprenant une couche logicielle à protéger.

Le procédé s'applique aussi dans un lecteur de type MP3 contenant une mémoire reprogrammable, tels que les lecteurs MP3 de type
15 clé USB.

REVENDICATIONS

1 - Procédé permettant de détecter et/ou d'éviter la modification de logiciels embarqués dans une mémoire programmable au sein d'un système comprenant un noyau dur contenant des fonctions de sécurité matérielle adaptées à vérifier l'intégrité d'un noyau mou comprenant une mémoire programmable, le système comportant une interface locale de données, caractérisé en ce qu'il comporte au moins les étapes suivantes :

A1 – le signal reçu sur l'interface locale de données n'est pas valide, mettre le système dans un état non opérationnel,

B1 – le signal reçu sur l'interface locale de données est un signal de déconnexion, ou il n'y a pas de signal, lancer une procédure de démarrage sécurisé, avec exécution des fonctions de contrôle :

Autotest du noyau dur :

- Si l'autotest est OK, alors tester l'intégrité de la mémoire reprogrammable,
 - Si cette intégrité est OK, alors activer le système pour un fonctionnement normal
 - Si cette intégrité est KO, alors mettre le système dans un état non opérationnel
- Si l'autotest est KO, alors mettre le système dans un état non opérationnel,

C1 – le signal reçu est un signal de démarrage valide,

- Si le système est dans un mode de développement, le rendre opérationnel,
- Si le système est dans un mode d'exploitation opérationnelle et si le signal est un signal de test, alors désactiver au moins une des fonctions essentielles du fonctionnement opérationnel.

2 - Procédé permettant de détecter et/ou d'éviter des modifications illicites d'un logiciel constructeur au sein d'un système de type GSM, comprenant un noyau dur et un noyau mou, une interface locale de données, comportant au moins les étapes suivantes :

A2 – le signal reçu sur l'interface locale de données du terminal n'est pas valide, mettre le terminal GSM dans un état non opérationnel,

B2 – le signal reçu sur l'interface locale de données est un signal de déconnexion, ou il n'y a pas de signal, lancer une procédure de démarrage sécurisé, avec exécution des fonctions de contrôle :

Autotest du noyau dur

- Si l'autotest est OK, alors tester l'intégrité du noyau mou
 - Si cette intégrité est OK, alors activer le terminal pour un fonctionnement normal,
 - Si l'intégrité est KO, alors mettre le terminal dans un état non opérationnel,
- Si l'autotest est KO, alors mettre le terminal GSM dans un état non opérationnel.

C2 – le signal reçu est un signal de démarrage valide :

- Si le fusible est non claqué, rendre le terminal GSM opérationnel,
- Si le fusible est claqué, rendre le terminal non totalement opérationnel, en désactivant au moins une des fonctions opérationnelles du terminal :
 - Si le signal est un signal de type test JTAG, poursuivre la procédure de test,
 - Si le signal est un signal de test, démarrer en mode non sécurisé et poursuivre la procédure de test.

3 – Procédé selon l'une des revendications 1 et 2 caractérisé en ce que l'échange des données entre le noyau dur et le noyau mou est effectué en utilisant un algorithme basé sur le principe de non-rejeu et de non-prédictibilité des données transmises.

4 – Système permettant de détecter et/ou d'éviter la modification de logiciels embarqués dans une mémoire programmable comprenant un noyau dur contenant des fonctions de sécurité matérielle et un noyau mou comprenant une mémoire programmable, une interface locale de données apte à recevoir des signaux, caractérisé en ce qu'il comporte des moyens adaptés à :

- mettre le système dans un état non opérationnel lorsque le signal reçu sur l'interface locale de données n'est pas valide,
- pour un signal reçu de déconnexion ou une absence de signal sur l'interface locale de données, lancer une procédure de démarrage sécurisé, avec exécution de fonctions de contrôle :

Autotest du noyau dur :

- Si l'autotest est OK, alors tester l'intégrité de la mémoire programmable,
 - Si cette intégrité est OK, alors activer le système pour un fonctionnement normal
 - Si cette intégrité est KO, alors mettre le système dans un état non opérationnel
- Si l'autotest est KO, alors mettre le système dans un état non opérationnel,
- Pour un signal reçu est un signal de démarrage valide,
- Si le système est dans un mode de développement, le rendre opérationnel,
- Si le système est dans un mode d'exploitation opérationnelle, et si le signal est un signal test alors désactiver au moins une des fonctions essentielles du fonctionnement opérationnel au démarrage.

5 – Système selon la revendication 4 caractérisé en ce qu'il comporte des moyens de sécurisation des échanges de données entre le noyau dur et le noyau mou.

6 – Système selon la revendication 4 caractérisé en ce que le système est un terminal GSM.

7 – Système selon la revendication 4 caractérisé en ce que le système est un micro-ordinateur.

8 – Système selon la revendication 4 caractérisé en ce que le système est un lecteur de type MP3 contenant une mémoire reprogrammable.

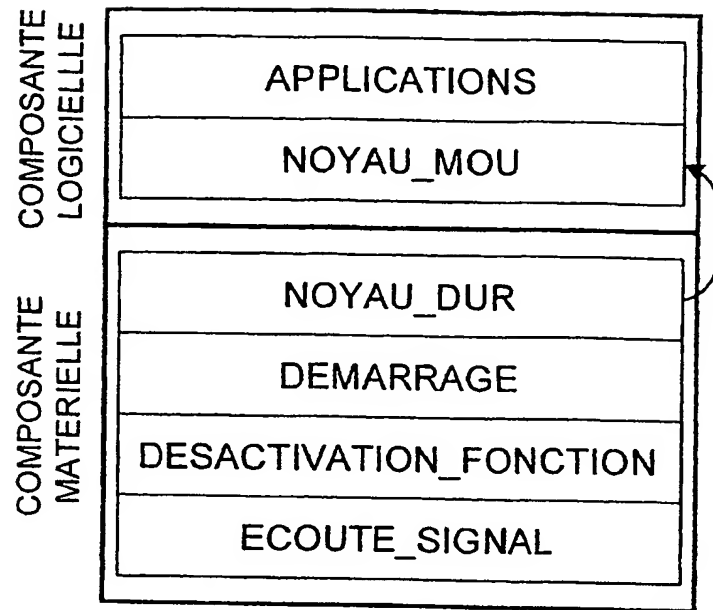


FIG. 1

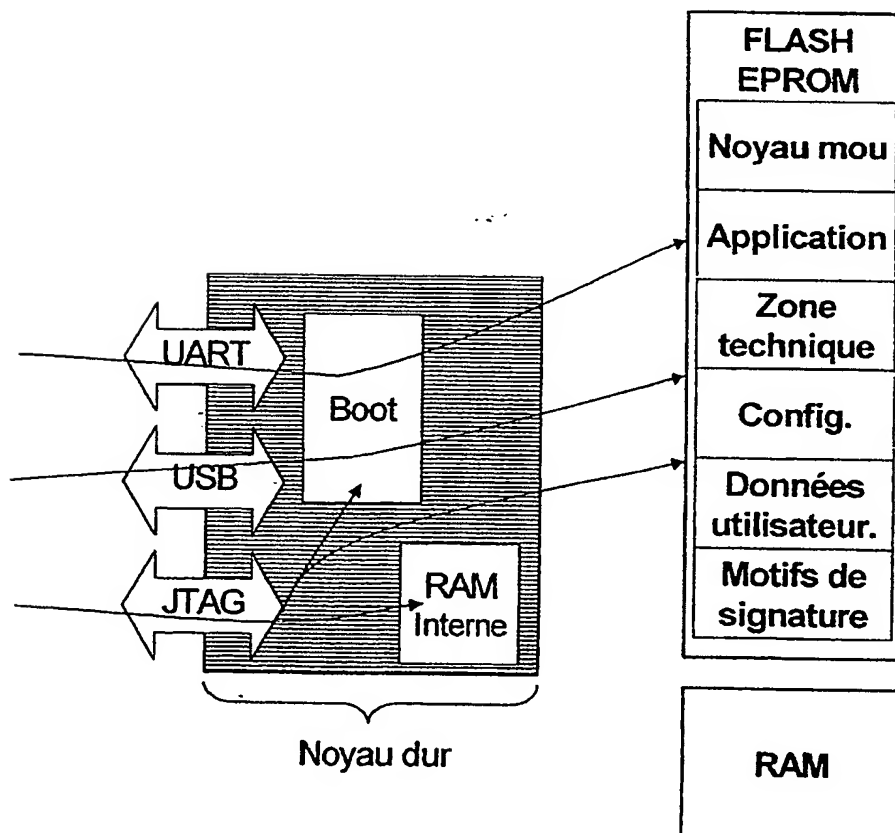


FIG. 2

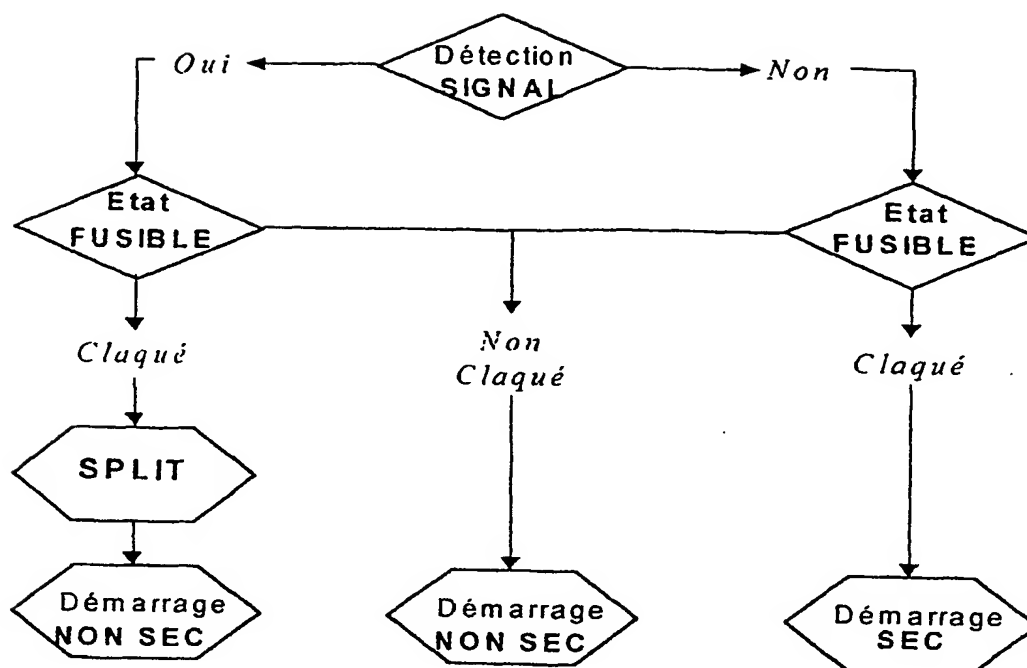


FIG.3

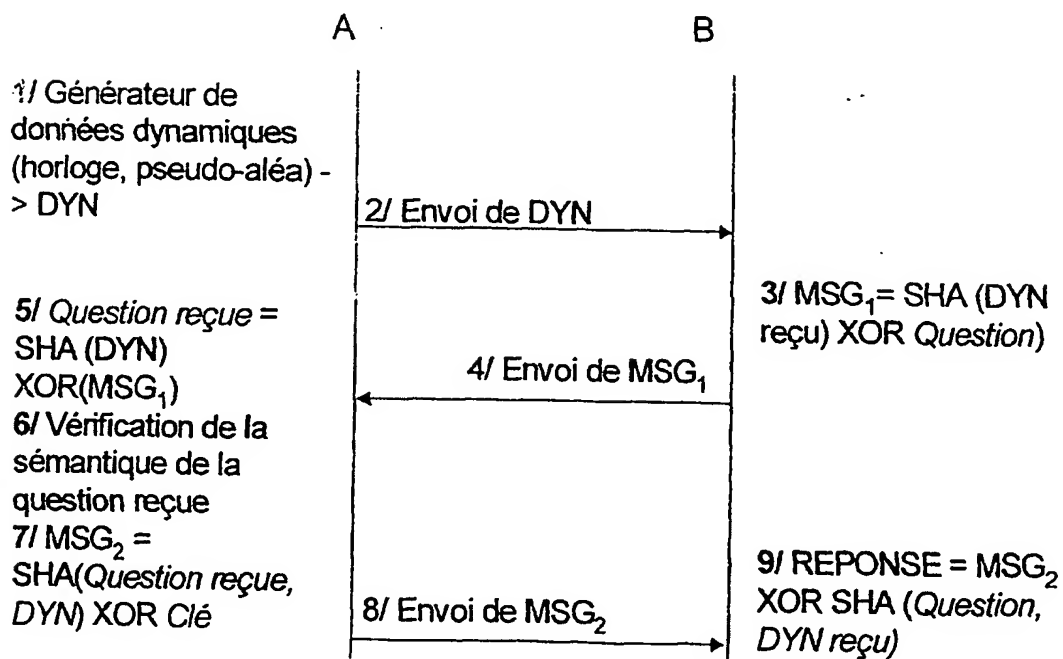


FIG.5

FIG.4

